

Table of Contents

Side-Channel Attacks

On the Simplicity of Converting Leakages from Multivariate to Univariate: Case Study of a Glitch-Resistant Masking Scheme	1
<i>Amir Moradi and Oliver Mischke</i>	
Success through Confidence: Evaluating the Effectiveness of a Side-Channel Attack	21
<i>Adrian Thillard, Emmanuel Prouff, and Thomas Roche</i>	
Profiling DPA: Efficacy and Efficiency Trade-Offs	37
<i>Carolyn Whitnall and Elisabeth Oswald</i>	
Non-invasive Spoofing Attacks for Anti-lock Braking Systems	55
<i>Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava</i>	

Physical Unclonable Function

An Accurate Probabilistic Reliability Model for Silicon PUFs	73
<i>Roel Maes</i>	
A High Reliability PUF Using Hot Carrier Injection Based Response Reinforcement	90
<i>Mudit Bhargava and Ken Mai</i>	
On the Effectiveness of the Remanence Decay Side-Channel to Clone Memory-Based PUFs	107
<i>Yossef Oren, Ahmad-Reza Sadeghi, and Christian Wachsmann</i>	

Lightweight Cryptography

Pushing the Limits of SHA-3 Hardware Implementations to Fit on RFID	126
<i>Peter Pessl and Michael Hutter</i>	
FIDES: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware	142
<i>Begül Bilgin, Andrey Bogdanov, Miroslav Knežević, Florian Mendel, and Qingju Wang</i>	

Hardware Implementations and Fault Attacks

On Measurable Side-Channel Leaks Inside ASIC Design Primitives 159
*Takeshi Sugawara, Daisuke Suzuki, Minoru Saeki,
Mitsuru Shiozaki, and Takeshi Fujino*

A Very High Speed True Random Number Generator with Entropy
Assessment 179
*Abdelkarim Cherkaoui, Viktor Fischer, Laurent Fesquet, and
Alain Aubert*

Stealthy Dopant-Level Hardware Trojans 197
*Georg T. Becker, Francesco Regazzoni, Christof Paar, and
Wayne P. Burleson*

A Differential Fault Attack on MICKEY 2.0 215
Subhadeep Banik and Subhamoy Maitra

Efficient and Secure Implementations

Improving Modular Inversion in RNS Using the Plus-Minus Method 233
Karim Bigou and Arnaud Tisserand

McBits: Fast Constant-Time Code-Based Cryptography 250
Daniel J. Bernstein, Tung Chou, and Peter Schwabe

Smaller Keys for Code-Based Cryptography: QC-MDPC McEliece
Implementations on Embedded Devices 273
Stefan Heyse, Ingo von Maurich, and Tim Güneysu

Sleuth: Automated Verification of Software Power Analysis
Countermeasures 293
Ali Galip Bayrak, Francesco Regazzoni, David Novo, and Paolo Ienne

Elliptic Curve Cryptography

Lambda Coordinates for Binary Elliptic Curves 311
*Thomaz Oliveira, Julio López, Diego F. Aranha, and
Francisco Rodríguez-Henríquez*

High-Performance Scalar Multiplication Using 8-Dimensional
GLV/GLS Decomposition 331
Joppe W. Bos, Craig Costello, Huseyin Hisil, and Kristin Lauter

On the Implementation of Unified Arithmetic on Binary Huff Curves . . . 349
Santosh Ghosh, Amit Kumar, Amitabh Das, and Ingrid Verbauwhede

Inverting the Final Exponentiation of Tate Pairings on Ordinary Elliptic Curves Using Faults	365
<i>Ronan Lashermes, Jacques Fournier, and Louis Goubin</i>	

Masking

Block Ciphers That Are Easier to Mask: How Far Can We Go?	383
<i>B. Gérard, Vincent Grosso, M. Naya-Plasencia, and François-Xavier Standaert</i>	
Masking vs. Multiparty Computation: How Large Is the Gap for AES?	400
<i>Vincent Grosso, François-Xavier Standaert, and Sebastian Faust</i>	
Analysis and Improvement of the Generic Higher-Order Masking Scheme of FSE 2012	417
<i>Arnab Roy and Srinivas Vivek</i>	

Side-Channel Attacks and Countermeasures

Using Bleichenbacher's Solution to the Hidden Number Problem to Attack Nonce Leaks in 384-Bit ECDSA	435
<i>Elke De Mulder, Michael Hutter, Mark E. Marson, and Peter Pearson</i>	
A New Model for Error-Tolerant Side-Channel Cube Attacks	453
<i>Zhenqi Li, Bin Zhang, Junfeng Fan, and Ingrid Verbauwhede</i>	
Leakage-Resilient Symmetric Encryption via Re-keying	471
<i>Michel Abdalla, Sonia Belaïd, and Pierre-Alain Fouque</i>	
Author Index	489